Linear codes from projective spaces

Michel Lavrauw, Leo Storme, and Geertrui Van de Voorde

Abstract. The linear code $C_{s,t}(n,q)$ of s-spaces and t-spaces in a projective space $\mathrm{PG}(n,q)$, $q=p^h$, p prime, is defined as the vector space spanned over $\mathbb{F}_p$ by the rows of the incidence matrix of s-spaces and t-spaces. This code generalises the code of points and lines in a projective plane, which has been intensively studied since the 1970's. In this paper, we give an overview of what is currently known about these codes and their duals.

1. Introduction

One of the important subjects in coding theory is the study of linear codes. A linear code C of *length* n and *dimension* k over a finite field $\mathbb{F}$ is a k-dimensional subspace of $\mathbb{F}^n$, and is often called a *linear* $[n,k]$ *code over* $\mathbb{F}$. Linear codes are *block codes* and besides their easy to grasp description, the advantages of linear codes lie in the algebraic structure of the code. In particular, they allow more efficient encoding and decoding algorithms compared to most other codes. The linear codes considered in this article are the codes that are generated by the rows of the incidence matrix of s-spaces and t-spaces of a projective space over a finite field (see Section 2.4). As a consequence, these codes inherit interesting properties from the geometric and combinatorial structure of the projective space they are constructed from.

The linear code of points and lines in a projective plane ($s=0$ and $t=1$) has been intensively studied and the nature of the codewords of minimum weight in this code has been known since the 1970's. In the late 1980's, the study of codewords of small weight and of the weight enumerator of codes from a projective plane turned out to be very useful in the computer proof of the non-existence of a projective plane of order 10 (see [**31**] for an overview of how Lam, Schwierz and Thiel found this proof). After that, codewords of small weight of (not necessarily Desarguesian) projective planes were studied and the minimum weight of the dual code arising from them was investigated.

Already in the 1970's, the code of points and t-spaces ($s=0$) was studied in a similar way, but apart from the determination of the codewords of minimum weight, not much was known. In 2002, the codes of points and t-spaces in $\mathrm{PG}(n,q)$

1991 *Mathematics Subject Classification.* 51E15, 51E20,94B05.

Key words and phrases. Linear codes, Projective spaces, Projective planes, Blocking sets, Unitals.

The first and the third author are supported by the Fund for Scientific Research – Flanders (FWO – Vlaanderen).

were generalised to codes of s-spaces and t-spaces in $\mathrm{PG}(n,q)$. In this article, we summarise what is presently known for these codes. We discuss the parameters of the code of s-spaces and t-spaces and of its dual code, and we give an overview of what is known about the codewords of small weight in the case that $s = 0$. We present a new upper bound on the minimum weight of the dual code of points and t-spaces in $\mathrm{PG}(n,q)$. For the planar case, we discuss the weight enumerator of the small planes, the codes of non-Desarguesian projective planes and the unitals contained in the code.

There are many open problems in the general case $s \neq 0$, but also in the easiest case (of points and lines in a projective plane) some important questions remain unanswered. For instance, the minimum weight of the dual code of the Desarguesian projective plane $\mathrm{PG}(2,q)$ is not known (except for the cases where q is prime or q is even).

2. Background and terminology

In this section, the necessary background for this survey is provided. Most of this is standard and can be found in the books [**24**] for projective spaces, [**25**] for projective planes, [**38**] for linear codes in general and [**2**] for linear codes from a projective space. The reader familiar with codes from projective spaces, may want to skip this introductory section.

2.1. Projective spaces over finite fields. In this paper, $\mathbb{F}_q$ will always denote the finite field with q elements where $q = p^h$, p prime, $h \geq 1$, and the symbols q, p and h will always be used in this sense. Let $\mathrm{V}(n+1,q)$ denote the vector space of dimension $n+1$ over $\mathbb{F}_q$.

The projective space $\mathrm{PG}(n,q)$ is the incidence structure with as points the vector spaces of rank 1 of $\mathrm{V}(n+1,q)$ and as lines the vector spaces of rank 2 of $\mathrm{V}(n+1,q)$. The *m-dimensional* subspaces of $\mathrm{PG}(n,q)$ correspond to vector subspaces of rank $m+1$ of $\mathrm{V}(n+1,q)$. The number of points in $\mathrm{PG}(n,q)$ is equal to $(q^{n+1}-1)/(q-1)$ and will be denoted by θ_n. The *Gaussian coefficient* $\begin{bmatrix} t \\ s \end{bmatrix}_q$ denotes the number of $(s-1)$-subspaces in $\mathrm{PG}(t-1,q)$, i.e.,

$$\begin{bmatrix} t \\ s \end{bmatrix}_q = \frac{(q^t-1)(q^{t-1}-1)\cdots(q^{t-s+1}-1)}{(q^s-1)(q^{s-1}-1)\cdots(q-1)}.$$

The subspaces of $\mathrm{PG}(n,q)$ of dimension $0, 1, 2$, and $n-1$ are called *points, lines, planes*, and *hyperplanes* respectively. A t-dimensional subspace is often called a *t-space*.

A *Baer subspace* of $\mathrm{PG}(n,q^2)$ is a subset isomorphic to $\mathrm{PG}(n,q)$.

2.2. Projective planes. A *projective plane* is a set of points and lines satisfying the following three axioms.

(A1) Through every two points, there is exactly one line.
(A2) Every two lines meet in exactly one point.
(A3) There exist four points, no three of which are collinear.

It is easy to prove that the number of points on a line in a projective plane is a constant; the *order* of a projective plane Π is the number of points on a line of Π minus one. The plane $\mathrm{PG}(2,q)$, arising from a 3-dimensional vector space over $\mathbb{F}_q$, is an example of a projective plane of order q. There are many kinds of projective

planes, some of which will be defined later in this section. Here we introduce two classes of projective planes: *Desarguesian* and *non-Desarguesian ones*. Two triangles $P_1P_2P_3$ and $R_1R_2R_3$ are said to be *in perspective* if the lines P_1R_1, P_2R_2 and P_3R_3 are concurrent, say in the point S. A plane is *Desarguesian* if for any two triangles $P_1P_2P_3$ and $R_1R_2R_3$ that are in perspective, the points $P_1P_2 \cap R_1R_2$, $P_1P_3 \cap R_1R_3$ and $P_2P_3 \cap R_2R_3$ are collinear. The Desarguesian planes are precisely the planes arising from a 3-dimensional vector space over a division ring, a result that already dates back to Hilbert [**23**]. In the finite case, using the theorem of Wedderburn [**37**] which states that a finite division ring is a field, this yields that a finite Desarguesian projective plane is necessarily a plane $\mathrm{PG}(2, q)$.

2.2.1. *Translation planes.* An *elation* with *axis* L and *center* P is a collineation (a mapping preserving incidence) that fixes all points on the line L and all lines through a point P, where P lies on L. The group of all elations with axis L and center P is denoted by $El(P, L)$. If for all lines $M \neq L$ through P, $El(P, L)$ acts transitively on the points of $M \setminus \{P\}$, $El(P, L)$ *is* (P, L)*-transitive*. A projective plane Π is called a *translation plane* if there exists a line L such that $El(P, L)$ is (P, L)-transitive for all points P of L. Translation planes are linked to spreads of the projective space via the André/Bruck-Bose construction [**1**],[**9**]. A $(t-1)$*-spread* of $\mathrm{PG}(n-1, q)$ is a partition of the projective space $\mathrm{PG}(n-1, q)$ in $(t-1)$-spaces. It can be proven that $\mathrm{PG}(n-1, q)$ admits a $(t-1)$-spread if and only if $t|n$ [**47**]. Let $\mathcal{S}$ be a $(t-1)$-spread in $\mathrm{PG}(2t-1, q)$. Embed $\mathrm{PG}(2t-1, q)$ as a hyperplane H in $\mathrm{PG}(2t, q)$. Let $\mathcal{P}$ be the set of points of $\mathrm{PG}(2t, q) \setminus H$, together with the $q^t + 1$ elements of $\mathcal{S}$. Let $\mathcal{L}$ be the set of t-spaces of $\mathrm{PG}(2t, q)$ intersecting H exactly in an element of $\mathcal{S}$, together with the space H itself. It is easy to check that if we take the elements of $\mathcal{P}$ as points, and the elements of $\mathcal{L}$ as lines and let a point P lie on a line L if $P \subseteq L$, we get a translation projective plane of order q^t.

A $(t-1)$*-regulus* is a set $\mathcal{R}$ of $q+1$ mutually skew $(t-1)$-spaces with the property that a line which meets three $(t-1)$-spaces of $\mathcal{R}$ meets all $(t-1)$-spaces of $\mathcal{R}$. The Desarguesian projective plane of order q^t is obtained from a *regular* $(t-1)$*-spread* $\mathcal{S}$ of $\mathrm{PG}(2t-1, q)$, which is a spread satisfying the condition that the regulus through three elements of $\mathcal{S}$ is completely contained in $\mathcal{S}$. It is shown that the Desarguesian projective planes are precisely those obtained from the André/Bruck-Bose construction starting from a regular spread [**9**].

For $t = 2$, there is a technique, called *derivation*, that enables us, starting from a translation plane of order q^2, to construct another projective plane of order q^2. This method is due to Ostrom [**41**] and works as follows. Let Π be a translation plane of order q^2, constructed via the André/Bruck-Bose construction from a spread $\mathcal{S}$ contained in $\mathrm{PG}(3, q)$. It is easy to see that, if $t = 2$, the *transversal lines*, which are the lines meeting all lines of a regulus $\mathcal{R}$, form a regulus too, called the *opposite regulus* $\mathcal{R}^{opp}$ of $\mathcal{R}$. If $\mathcal{S}$ is a 1-spread containing a regulus, then let $\mathcal{D}_{\mathcal{S}}(\mathcal{R})$ be the spread obtained from $\mathcal{S}$ by replacing the lines of a regulus $\mathcal{R}$ by $\mathcal{R}^{opp}$. The plane of order q^2 obtained via the André/Bruck-Bose construction of the spread $\mathcal{D}_{\mathcal{S}}(\mathcal{R})$ is again a translation plane, called the *derived plane of* Π.

2.2.2. *Figueroa planes.* Consider the plane $\mathrm{PG}(2, q^3)$. Applying the automorphism $\sigma : x \mapsto x^q$ to all coordinates induces a collineation of $\mathrm{PG}(2, q^3)$, fixing a subplane $\pi = \mathrm{PG}(2, q)$. Let S be the set of points P such that $P, P^\sigma, P^{\sigma^2}$ are not collinear (these are exactly the points lying on no secant lines to π) and let T be the set of lines L of $\mathrm{PG}(2, q^3)$ such that L, L^σ and L^{σ^2} are not concurrent. We now

define a bijection μ between the points of S and the lines of T. Let

$$P^\mu = P^\sigma P^{\sigma^2}, \forall P \in S,$$

$$L^\mu = L^\sigma \cap L^{\sigma^2} \forall L \in T.$$

Let $\mathcal{P}$ be the set of points of $\mathrm{PG}(2, q^3)$ and let $\mathcal{L}$ be the set of lines of $\mathrm{PG}(2, q^3)$. We change the incidence relation I of $\mathrm{PG}(2, q^3)$ to the following relation:

$$PI'L \iff \begin{cases} L^\mu I P^\mu & \text{if } P \in S \text{ and } L \in T, \\ PIL & \text{otherwise.} \end{cases}.$$

The set of points and lines of $\mathrm{PG}(2, q^3)$, together with the incidence relation I′, yields a projective plane of order q^3. This plane is called the *Figueroa* plane [**16**] of order q^3 and is non-Desarguesian for $q > 2$.

2.2.3. *Projective planes of order 9.* It is known that the projective planes of orders $2, 3, 4, 5, 7, 8$ are unique, and hence, Desarguesian (for the planes of order 7 or 8, see [**21**],[**22**]). Lam, Kolesova and Thiel obtained a computer assisted proof of the fact that there are exactly 4 projective planes of order 9 [**33**]. Obviously, $\mathrm{PG}(2, 9)$ is one of these four planes. The derived plane of $\mathrm{PG}(2, 9)$ is called the *Hall plane*, which is non-Desarguesian (see e.g. [**25**, p. 210]). When switching points and lines in the Hall plane, we obtain the *dual Hall plane*, which can be shown to be non-Desarguesian and non-isomorphic to the Hall plane itself. The fourth plane of order 9 is the *Hughes plane of order 9*. For the description of the Hughes planes $Hu(q^2)$ of order q^2, where q is odd, we follow [**14**, p. 725]. Consider the set $V = \{(x, y, z) | x, y, z \in \mathbb{F}_{q^2}\}$. Define addition $+$ on V componentwise and define a left scalar multiplication by the elements of $\mathbb{F}_{q^2}$ by $k \circ (x, y, z) = (k \circ x, k \circ y, k \circ z)$, where $x \circ y = xy$ if xy is a square and $x \circ y = xy^q$ if xy is a non-square. Both the points and the lines of $Hu(q^2)$ are subsets of $\mathbb{F}_{q^2}^3 \setminus \{(0, 0, 0)\}$ and $\langle x, y, z\rangle$ represents $\{(k \circ x, k \circ y, k \circ z) | k \in \mathbb{F}_{q^2}^*\}$. The points of $Hu(q^2)$ can be identified with the points of $\mathrm{PG}(2, q^2)$. Incidence is determined as follows. Fix a basis $\{1, t\}$ for $\mathbb{F}_{q^2}$ as a vector space over $\mathbb{F}_q$. Let $\langle x, y, z\rangle$ be a point of $\mathrm{PG}(2, q^2)$ and let $\langle u, v, w\rangle$ be a line of $\mathrm{PG}(2, q^2)$, with $u = u_1 + tu_2, v = v_1 + tv_2, w = w_1 + tw_2$. Then $\langle u, v, w\rangle$ and $\langle x, y, z\rangle$ are incident if and only if $xu_1 + yv_1 + zw_1 + (xu_2 + yv_2 + zw_2) \circ t = 0$. The Hughes plane of order 9 was already introduced in 1907 in [**50**], it is not a translation plane and it is self-dual. By the result of Lam, Schwiez and Thiel, there are no other projective planes of order 9 [**32**].

2.3. Some subsets of projective spaces.

2.3.1. *k-Blocking sets.* A *k-blocking set* B in $\mathrm{PG}(n, q)$ is a set of points such that any $(n - k)$-dimensional subspace intersects B and B is called *trivial* when a k-dimensional subspace is contained in B. A k-blocking set is also referred to as a *blocking set with respect to $(n - k)$-spaces*. A 1-blocking set in $\mathrm{PG}(n, q)$ is simply called a blocking set in $\mathrm{PG}(n, q)$.

If an $(n - k)$-dimensional space contains exactly one point of a k-blocking set B in $\mathrm{PG}(n, q)$, it is called a *tangent $(n-k)$-space* to B, and a point $P \in B$ is called *essential* when it belongs to a tangent $(n - k)$-space of B. A k-blocking set B is called *minimal* when no proper subset of B is also a k-blocking set, i.e., when each point of B is essential. A k-blocking set B is called *small* if $|B| < 3(q^k + 1)/2$.

A *Rédei-type* k-blocking set in $\mathrm{PG}(n, q)$ is a blocking set B such that there exists a hyperplane with $|B| - q^k$ points.

The construction of a codeword of low weight in $\mathrm{C}_k(n,q)^\perp$ relies on the following theorem.

THEOREM 2.1. [**49**, Theorem 2.7] *Let B be a small minimal k-blocking set of* $\mathrm{PG}(n,q)$. *Then any subspace that intersects B, intersects it in* $1 \mod p$ *points.*

2.3.2. *Ovals and hyperovals.* An *oval* $\mathcal{O}$ in $\mathrm{PG}(2,q)$ is a set of $q+1$ points, no three of which are collinear. A *tangent line* to an oval $\mathcal{O}$ is a line containing exactly one point of $\mathcal{O}$, a *secant line* is a line meeting $\mathcal{O}$ in two points and an *external line* is a line not containing a point of $\mathcal{O}$. The following lemma can be found in [**24**].

LEMMA 2.2. [**24**, Lemma 8.6] *The tangent lines to an oval $\mathcal{O}$ in* $\mathrm{PG}(2,q)$ *are concurrent if q is even.*

Using Lemma 2.2, we see that every oval $\mathcal{O}$ in $\mathrm{PG}(2,q)$, q even, can be extended by the common point n of all tangent lines to $\mathcal{O}$ to a larger oval. The point n is called the *nucleus* of $\mathcal{O}$ and the set $\mathcal{O} \cup \{n\}$ is a *hyperoval*, where a hyperoval is defined as a set of $q+2$ points, no three of which are collinear. It is easy to see that hyperovals only exist for q even.

It is clear that a non-degenerate conic is an oval.The following famous theorem is due to Segre and states that if q is odd, the converse is true, thus linking the intersection properties of an oval to its algebraic properties.

THEOREM 2.3. [**46**] *If q is odd, every oval of* $\mathrm{PG}(2,q)$ *is a conic.*

From Lemma 2.2, it follows that a conic in $\mathrm{PG}(2,q)$, q even, together with its nucleus, form a hyperoval. The hyperovals arising in this way are called *regular* hyperovals. A regular hyperoval can be written as the set of points $\{(1,t,t^2)|t \in \mathbb{F}_q\} \cup \{(0,0,1)\} \cup \{(0,1,0)\}$. Replacing t^2 by t^{2^v}, where $\gcd(v,h)=1$, yields a class of hyperovals, called *translation hyperovals*. Other infinite families of hyperovals are known. Classifying hyperovals is a hard problem and the classification of hyperovals remains open for $q \geq 64$ [**42**].

2.3.3. *Unitals.* A *unital* of $\mathrm{PG}(2,q)$, q square, is a set $\mathcal{U}$ of $q\sqrt{q}+1$ points such that every line contains 1 or $\sqrt{q}+1$ points of $\mathcal{U}$. Let q be a square and let

$$H(X) = \sum_{i,j=0}^{2} a_{ij} X_i X_j^{\sqrt{q}},$$

with $a_{ij} = a_{ji}^{\sqrt{q}}$, a Hermitian form over $\mathbb{F}_q$. A *Hermitian curve* in $\mathrm{PG}(2,q)$, denoted by $\mathcal{H}(2,q)$, is a set of points whose coordinates, with respect to a fixed basis, satisfy $H(X)=0$. A non-degenerate Hermitian curve is an example of a unital, and a unital arising from a Hermitian curve is called a *Hermitian unital* (or *classical* unital).

2.4. The linear code of s-spaces and t-spaces in $\mathrm{PG}(n,q)$**.** A p-ary *linear code* C of *length* m and dimension k is a k-dimensional linear subspace of $V(m,p)$, where $V(m,p)$ denotes the m-dimensional vector space over $\mathbb{F}_p$, p prime. A *codeword* is a vector of C. A *generator matrix* G for a linear code C is a matrix whose rows form a basis of C.

The *support* of a codeword c, denoted by $supp(c)$, is the set of all non-zero positions of c. The *weight* of c is the number of non-zero positions of c and is denoted by $wt(c)$. The *minimum weight* of a linear code C is equal to $\min\{wt(c)|c \in$

$\mathrm{C} \setminus \{0\}\}$. The *weight distribution* of a code C with length n is the set $\{A_0, \ldots, A_n\}$, where A_i denotes the number of codewords in C with weight i. The *(Hamming) distance* between two codewords c and c', denoted by $d(c, c')$, is equal to the number of positions in which the corresponding coordinates are different. The *minimum distance* $d(\mathrm{C})$ of C is equal to $\min\{d(c, c')|c, c' \in \mathrm{C}, c \neq c'\}$. The minimum distance determines the number of errors that can be detected and corrected using this code, when using *nearest-neighbour-decoding*. This method decodes a received vector to the codeword that is nearest to it in terms of Hamming distance. If C is a linear code with minimum distance d then C can detect up to $d-1$ errors and correct up to $\lfloor (d-1)/2 \rfloor$ errors. It is easy to see that in a linear code, the minimum weight and the minimum distance are equal. A linear code C with length m, dimension k and minimum distance d is often called an $[m, k, d]$-code.

The *dual code* $\mathrm{C}^\perp$ of a p-ary linear code C of length m is the set of all vectors orthogonal to all codewords of C, hence

$$\mathrm{C}^\perp = \{v \in V(m, p) | (v, c) = 0, \ \forall c \in \mathrm{C}\}.$$

We define the *incidence matrix* $A = (a_{ij})$ of s-spaces and t-spaces in the projective space $\mathrm{PG}(n, q)$ as the matrix whose rows are indexed by the t-spaces of $\mathrm{PG}(n, q)$ and whose columns are indexed by the s-spaces of $\mathrm{PG}(n, q)$, and with entry

$$a_{ij} = \begin{cases} 1 & \text{if } s\text{-space } j \text{ is contained in } t\text{-space } i, \\ 0 & \text{otherwise.} \end{cases}$$

The p-ary *linear code of s-spaces and t-spaces* of $\mathrm{PG}(n, q)$, $q = p^h$, p prime, $h \geq 1$, is the code generated by the rows of the incidence matrix of s-spaces and t-spaces in $\mathrm{PG}(n, q)$ and is denoted by $\mathrm{C}_{s,t}(n, q)$. In the particular case that $s = 0$, we denote the p-ary linear code of points and t-spaces of $\mathrm{PG}(n, q)$, $q = p^h$, by $\mathrm{C}_t(n, q)$. The p-ary code of points and lines of a projective plane Π will be denoted by $\mathrm{C}(\Pi)$, and in the case that $\Pi = \mathrm{PG}(2, q)$, by $\mathrm{C}(2, q)$.

In what follows, we often identify the support of a codeword of $\mathrm{C}_k(n, q)$ with the corresponding set of points of $\mathrm{PG}(n, q)$. Furthermore, if T is a set of points of $\mathrm{PG}(n, q)$, then the incidence vector of this set is also denoted by T.

The parameters s, t and n will always satisfy $n \geq 2$, $0 \leq s < t \leq n-1$ unless indicated differently.

The code $\mathrm{C}_{s,t}$ was introduced as a generalisation of the code of points and lines in a projective plane. Another code C' of s-spaces and t-spaces in $\mathrm{PG}(n, q)$ can be obtained if we change the definition of the incidence matrix. We can put a 1 in the position a_{ij} if s-space j and t-space i have a non-trivial intersection. This code has known dimension [**48**], but no other results are known, except for the case $s = 0$, where C' coincides with $\mathrm{C}_t(n, q)$.

Open Problem 2.4. Determine the minimum weight of the code $\mathrm{C}'_{s,t}$ defined above, for $s \neq 0$.

The code $\mathrm{C}_{s,t}(n, q)$ is always taken p-ary (if $q = p^h$), and one might wonder why these codes are not always taken over $\mathbb{F}_2$, or over some other finite field. The reason why the only interesting codes are the p-ary codes, where p divides the order of the projective space, is shown in the following theorem. The proof given here is a straightforward extension of the proof given in [**11**, Proposition 8] for the case of finite projective planes. This theorem also holds for non-Desarguesian planes

and for (putative) planes of which the order is not a prime power. Recall that θ_t denotes the number of points in $\mathrm{PG}(t,q)$, i.e. $\theta_t = (q^{t+1}-1)/(q-1)$.

THEOREM 2.5. *Let* C *be the p-ary code of points and t-spaces in a projective space $\Pi = \mathrm{PG}(n,q)$ of order q, where $p \nmid q$. Then* C *is either the $[\theta_n, \theta_n - 1, 2]$-code which is the dual of the all-one vector* $\mathbf{1}$*, or* C *is the $[\theta_n, \theta_n, 1]$-code which is the entire vector space.*

PROOF. Let π_i be the t-spaces contained in $\mathrm{PG}(n,q)$, then $c = \sum_i \pi_i = \begin{bmatrix} n \\ t \end{bmatrix} \mathbf{1}$ is a codeword of the p-ary code C of points and t-spaces of $\mathrm{PG}(n,q)$. Let c^x be the codeword which is the sum of all t-spaces through a point x. The codeword $c^{xy} := c^x - c^y$, for $x \neq y$, has $c^{xy}_x = \begin{bmatrix} n \\ t \end{bmatrix} - \begin{bmatrix} n-1 \\ t-1 \end{bmatrix}$, $c^{xy}_y = -\begin{bmatrix} n \\ t \end{bmatrix} + \begin{bmatrix} n-1 \\ t-1 \end{bmatrix}$ and $c^{xy}_z = 0$ for all $z \neq x, y$. Hence, codewords c^{xy}, with $x \neq y$, clearly belong to the code $\mathbf{1}^\perp$. It is easy to see that the code $\mathbf{1}^\perp$ has dimension at most $\theta_n - 1$. Since $\{c^{xy} | y \neq x\}$ is a set of $\theta_n - 1$ independent codewords, contained in $\mathbf{1}^\perp$, the dimension of $\mathbf{1}^\perp$ is equal to $\theta_n - 1$. The generators c^{xy}, $y \neq x$, of the code $\mathbf{1}^\perp$, are contained in C, hence, $\mathbf{1}^\perp \subseteq$ C and the theorem follows. □

3. The code $\mathrm{C}_{s,t}(n,q)$

3.1. The parameters of $\mathrm{C}_{s,t}(n,q)$. As seen in Section 2.4, the length m of linear code C determines the number of symbols that are used to transmit one codeword, the dimension k determines how many different codewords there are in C, and the minimum distance d determines the number of errors that can be corrected using the code C. One of the main problems in the theory of linear codes is to find the parameters m, k and d of a certain code. In this section we discuss the parameters of the code $\mathrm{C}_{s,t}(n,q)$. It follows from the definition that the dimension of the code $\mathrm{C}_{s,t}(n,q)$ is equal to the rank of the incidence matrix of s-spaces and t-spaces, considered over $\mathbb{F}_p$, i.e. the *p-rank* of this incidence matrix.

Clearly, the length of $\mathrm{C}_{s,t}(n,q)$ is the number of s-spaces in $\mathrm{PG}(n,q)$, i.e. $\begin{bmatrix} n+1 \\ s+1 \end{bmatrix}_q$. In 2002, Bagchi and Inamdar determined the minimum weight and the nature of the minimum weight codewords of $\mathrm{C}_{s,t}(n,q)$ resulting in the following theorem. Let $\Delta_{s,t}$ denote the incidence system whose points and blocks are the s-spaces and t-spaces in $\mathrm{PG}(n,q)$, respectively, and the incidence is inclusion.

THEOREM 3.1. [**6**, Theorem 1] *The minimum weight of $\mathrm{C}_{s,t}(n,q)$ is $\begin{bmatrix} t+1 \\ s+1 \end{bmatrix}_q$, and the minimum weight vectors are the scalar multiples of incidence vectors of the blocks of $\Delta_{s,t}$.*

For $\mathrm{C}_t(n,q)$, this result was known since the 1970's in which Theorem 3.1 reduces to the following theorem.

THEOREM 3.2. [**2**, Proposition 5.7.3] *The minimum weight codewords of $\mathrm{C}_t(n,q)$ are the scalar multiples of the incidence vectors of the t-spaces.*

The dimension of this code is only known for the case of points and t-spaces in $\mathrm{PG}(n,q)$. The dimension of $\mathrm{C}_k(n,q)$ is determined by Hamada in [**20**], where he gives the following formula.

THEOREM 3.3. [**20**] *The dimension of the p-ary code $\mathrm{C}_t(n,q)$, $q=p^h$, is given by:*

$$\sum_{s_0}\cdots\sum_{s_{h-1}}\prod_{j=0}^{h-1}\sum_{i=0}^{L(s_{j+1},s_j)}(-1)^i\binom{t+1}{i}\binom{t+s_{j+1}p-s_j-ip}{t},$$

where $s_h=s_0$ and summations are taken over all integers s_j (for $j=0,\ldots,h-1$) such that

$$r+1\leq s_j\leq t+1,\ \textit{and}\ 0\leq s_{j+1}p-s_j\leq(t+1)(p-1),$$

and

$$L(s_{j+1},s_j)=\lfloor\frac{s_{j+1}p-s_j}{p}\rfloor.$$

In [**26**], the authors prove the following slightly easier formula for the dimension of the code $\mathrm{C}_t(n,q)$.

THEOREM 3.4. [**26**, Theorem 2.13] *The dimension of the p-ary code $\mathrm{C}_t(n,q)$, $q=p^h$, is given by:*

$$1+\sum_{i=1}^{n-t}\sum_{\substack{1\leq r_1,\ldots,r_{l-1}\leq n-t\\ r_0=r_l=i}}\prod_{j=0}^{h-1}\sum_{s=0}^{r_{j+1}-1}(-1)^s\binom{n+1}{s}\binom{n+pr_{j+1}-r_j-ps}{n}.$$

In the case of points and hyperplanes, this formula simplifies to the following formula, which was already deduced by Goethals and Delsarte [**18**].

THEOREM 3.5. [**18**] *The dimension of the p-ary code $\mathrm{C}_{n-1}(n,q)$, $q=p^h$, is*

$$\binom{n+p-1}{n}^h+1.$$

It follows from the previous theorem that the p-rank of the incidence matrix of points and lines of $\mathrm{PG}(2,q)$, $q=p^h$ is $\binom{p+1}{2}^h+1$. This was already proved in 1966 by Graham and MacWilliams [**19**]. Hamada and Sachar conjecture that Desarguesian projective planes can be characterised by this property.

OPEN PROBLEM 3.6. Show that the incidence matrix of every projective plane π of order p^h has p-rank at least $\binom{p+1}{2}^h+1$ and that equality holds if and only if the plane π is Desarguesian.

Moreover, Salwach showed that the p-rank of the incidence matrix of an arbitrary projective plane of order p, p prime, is $\binom{p+1}{2}+1$ [**45**]. Thus, if one can prove the Hamada-Sachar conjecture, one has proved another - more famous - conjecture, namely the conjecture that the projective plane of order p is unique.

OPEN PROBLEM 3.7. Determine the dimension of $\mathrm{C}_{s,t}(n,q)$, $s\neq 0$.

For the binary code $\mathrm{C}_{s,s+2}(n,q)$, McClurg derived an upper bound on the dimension in [**39**].

3.2. Codewords of small weight in $\mathrm{C}_{s,t}(n,q)$. For some small planes, the entire weight distribution of the code $\mathrm{C}(2,q)$ is known. Recall that A_i denotes the number of codewords with weight i.

3.2.1. *The projective plane of order* 2. This code has parameters $[7, 4, 3]$ and $A_0 = 1, A_3 = 7, A_4 = 7, A_7 = 1$ and all other $A_i = 0$. This code is the well-known Hamming code $Ham(3, 2)$.

3.2.2. *The projective plane of order* 3. This code has parameters $[13, 7, 4]$ and $A_0 = 1, A_4 = 26, A_6 = 156, A_7 = 624, A_9 = 494, A_{10} = 780, A_{12} = 78, A_{13} = 28$ and all other $A_i = 0$.

3.2.3. *The projective plane of order* 4. This code has parameters $[21, 10, 5]$. Its weight distribution is $A_0 = A_{21} = 1, A_5 = A_{16} = 21, A_8 = A_{13} = 210, A_9 = A_{12} = 280$ and all other $A_i = 0$.

3.2.4. *The projective plane of order* 5. This code has parameters $[31, 16, 6]$. The weight enumerator was determined by hand in [**40**]. They found that the weight distribution is:

$A_0 = 1$	$A_{16} = 41085540$	$A_{24} = 24062665000$
$A_6 = 124$	$A_{17} = 148242000$	$A_{25} = 27302369724$
$A_{10} = 1860$	$A_{18} = 465620000$	$A_{26} = 25006057620$
$A_{11} = 5580$	$A_{19} = 1279819500$	$A_{27} = 18607471000$
$A_{12} = 62000$	$A_{20} = 3020794380$	$A_{28} = 10587941500$
$A_{13} = 604500$	$A_{21} = 6454257660$	$A_{29} = 4408386000$
$A_{14} = 1767000$	$A_{22} = 11506425000$	$A_{30} = 1165216220$
$A_{15} = 11895940$	$A_{23} = 18365221500$	$A_{31} = 151980976,$

and all other $A_i = 0$.

3.2.5. *The projective plane of order* 8. This code has parameters $[73, 28, 9]$. Prange [**43**] calculated its weight enumerator by computer in 1959, and Chouinard [**11**] by hand in 2000. They found:

$A_0 = A_{73} = 1$	$A_{28} = A_{45} = 6671616$
$A_9 = A_{64} = 73$	$A_{29} = A_{44} = 10596096$
$A_{16} = A_{57} = 2628$	$A_{32} = A_{41} = 29369214$
$A_{21} = A_{52} = 56064$	$A_{33} = A_{40} = 36301440$
$A_{24} = A_{49} = 784896$	$A_{36} = A_{37} = 49056000$
$A_{25} = A_{48} = 1379700,$	and all other $A_i = 0$.

In all other cases, only partial results are known. The search for small weight codewords started in the 1990's, and the first results were obtained for the code of points and lines of planes of prime order. McGuire and Ward [**40**] proved that there are no codewords of $\mathrm{C}(2, p)$, p an odd prime, in the interval $[p+2, 3(p+1)/2]$. This result was extended by Chouinard in [**11**], [**12**], where he proved the following theorem.

THEOREM 3.8. [**11**],[**12**] *There are no codewords in* $\mathrm{C}(2, p)$*, p prime, with weight in the closed interval* $[p + 2, 2p - 1]$.

In [**15**], the result of Chouinard was extended by Fack et al. to a larger interval for p prime.

THEOREM 3.9. [**15**, Theorem 4] *The only codewords c, with* $0 < wt(c) \leq 2p + (p - 1)/2$*, in* $\mathrm{C}(2, p)$*, $p \geq 11$, are:*

(i) *codewords with weight* $p + 1$*: $\alpha\ell$, with ℓ a line of* $\mathrm{PG}(2, p)$*,* $\alpha \in \mathbb{F}_p \setminus \{0\}$*,*
(ii) *codewords with weight* $2p : \alpha(\ell_1 - \ell_2)$*, with ℓ_1 and ℓ_2 two distinct lines of* $\mathrm{PG}(2, p)$*,* $\alpha \in \mathbb{F}_p \setminus \{0\}$*,*
(iii) *codewords with weight* $2p + 1$*: $\alpha\ell_1 + \beta\ell_2$,* $\beta \neq -\alpha$*,* $\alpha, \beta \in \mathbb{F}_p \setminus \{0\}$*, with ℓ_1 and ℓ_2 two distinct lines of* $\mathrm{PG}(2, p)$*.*

Very recently, this theorem was improved by Gács, Szőnyi and Weiner in [**17**] who proved the following result.

THEOREM 3.10. [**17**] *A codeword c in $\mathrm{C}(2,q)$, $q=p^h$, with $wt(c) < \lceil\sqrt{q}\rceil q + 1 + (q - \lceil\sqrt{q}\rceil^2)$ is a linear combination of $\lceil\frac{wt(c)}{q+1}\rceil$ lines, when q is large and $h>2$.*

We believe that the techniques developed by Gács, Szőnyi and Weiner to prove Theorem 3.10 might be extendable to find similar results for the code $\mathrm{C}_k(n,q)$. This makes it very plausible that in the near future, codewords of small weight in $\mathrm{C}_k(n,q)$ will be characterised up to much larger weights. The following result is already known.

THEOREM 3.11. [**36**, Theorem 12] *There are no codewords in $\mathrm{C}_t(n,q)\backslash\mathrm{C}_{n-t}(n,q)^\perp$, $q=p^h$, with weight in the open interval $]\theta_t, 2q^t[$, $p>5$.*

Theorem 3.11 does not say anything about the codewords that are contained in $\mathrm{C}_t(n,q)\cap\mathrm{C}_{n-t}(n,q)^\perp$. In the next theorem, these kinds of codewords are permitted.

THEOREM 3.12. *There are no codewords in $\mathrm{C}_t(n,q)$, $q=p^h$, with weight in the open interval $]\theta_t, 2(\frac{q^n-1}{q^t-1}(1-\frac{1}{p})+\frac{1}{p})[$.*

OPEN PROBLEM 3.13. Characterise codewords of weight smaller than a certain constant in $\mathrm{C}_t(n,q)$, $n>2$, as a linear combination of codewords of minimum weight.

The following theorem shows that there is an empty interval on the size of small weight codewords of $\mathrm{C}_{n-1}(n,q)$. This interval is sharp since θ_{n-1} is the weight of a codeword arising from the incidence vector of a hyperplane and $2q^{n-1}$ is the weight of a codeword arising from the difference of the incidence vectors of two distinct hyperplanes.

THEOREM 3.14. [**36**, Corollary 20] *There are no codewords with weight in the open interval $]\theta_{n-1}, 2q^{n-1}[$ in the code $\mathrm{C}_{n-1}(n,q)$, $q=p^h$, $p>5$.*

Also in the prime case, we have a sharp interval.

THEOREM 3.15. [**36**, Corollary 21] *There are no codewords with weight in the open interval $]\theta_t, 2p^t[$ in the code $\mathrm{C}_t(n,p)$, $p>5$.*

OPEN PROBLEM 3.16. Determine whether there is a gap in the weight enumerator of the code $\mathrm{C}_{s,t}(n,q)$.

3.3. The Hermitian unitals as codewords. It follows from the following result that Hermitian unitals are codewords in $\mathrm{C}(2,q^2)$.

THEOREM 3.17. [**2**, Theorem 6.6.1] *The code of points and Hermitian unitals in $\mathrm{PG}(2,q^2)$ equals the code of points and lines in $\mathrm{PG}(2,q^2)$.*

This theorem shows the sharpness of the bound in Theorem 3.10. In [**7**], Blokhuis et al. prove the following theorem, conjectured by Assmus and Key in [**3**].

THEOREM 3.18. *Let U be a unital embedded in $\Pi=\mathrm{PG}(2,q^2)$, then U is Hermitian if and only if the incidence vector of U is in $\mathrm{C}(\Pi)$.*

It follows from this theorem that a Hermitian unital can be written as a sum of lines.

OPEN PROBLEM 3.19. Determine the linear combination of lines that gives the Hermitian unital.

In 2003, Baker and Wantz extended this theorem for a particular class of unitals in the Hughes plane [**5**].

4. The code $\mathrm{C}_{s,t}(n,q)^\perp$

4.1. The parameters of $\mathrm{C}_k(n,q)^\perp$. In this section, we summarise the known results on the parameters of the dual code $\mathrm{C}_{s,t}(n,q)^\perp$ of $\mathrm{C}_{s,t}(n,q)$. In contrast to the previous case, the minimum weight of the dual code $\mathrm{C}_{s,t}(n,q)^\perp$ is not known, and even for the case $\mathrm{C}(2,q)^\perp$, only bounds on the minimum weight are known (unless q is even or prime).

We first give a construction of a codeword of $\mathrm{C}_{s,t}(n,q)^\perp$ of small weight. Recall that by hypothesis, $s < t$. Let μ_1 and μ_2 be two $(n-t+s)$-spaces in $\mathrm{PG}(n,q)$ intersecting in an $(n-t+s-1)$-dimensional space μ. Let π be an $(s-1)$-dimensional subspace of μ. Let $\mathcal{S}$ be the set of s-spaces through π contained in $(\mu_1 \cup \mu_2)$, not lying in μ. Then $\mathcal{S}$ corresponds to a codeword of weight $2q^{n-t}$ in $\mathrm{PG}(n,q)$. This observation gives an upper bound on the minimum weight of $\mathrm{C}_{s,t}(n,q)^\perp$. In [**6**], Bagchi and Inamdar derive the following lower bound on $d(\mathrm{C}_{s,t}(n,q)^\perp)$.

THEOREM 4.1. [**6**, Theorem 3] *The minimum weight d of $\mathrm{C}_{s,t}(n,q)^\perp$ satisfies:*

$$2\left(\frac{q^{n-s}-1}{q^{t-s}-1}(1-\frac{1}{p})+\frac{1}{p}\right) \leq d \leq 2q^{n-t}.$$

If the lower bound is attained, then $t = s+1$.

It is easy to see that for q prime and $t = s+1$, the upper and lower bound in the previous theorem coincide, hence, the minimum weight of $\mathrm{C}_{s,s+1}(n,p)^\perp$, p prime, is equal to $2p^{n-s-1}$. In the case that $s = 0$, Bagchi and Inamdar also determine the nature of the codewords of minimum weight $2p^{n-1}$ in $\mathrm{C}_1(n,p)^\perp$.

THEOREM 4.2. [**6**, Proposition 2] *The minimum weight of $\mathrm{C}_1(n,p)^\perp$, p prime, is $2p^{n-1}$. Moreover, the codewords of minimum weight are precisely the scalar multiples of the difference of two hyperplanes.*

The fact that the minimum weight of $\mathrm{C}(2,p)^\perp$, p prime, is $2p$ was already known since the 1970's, when Assmus and Key derived the following bounds on the minimum weight of $\mathrm{C}(2,q)^\perp$.

THEOREM 4.3. [**2**, Theorem 6.4.2] *The minimum weight d of $\mathrm{C}(2,q)^\perp$ satisfies*

$$q+p \leq d \leq 2q,$$

and the lower bound is attained if $p = 2$.

The sharpness of the lower bound follows from the existence of hyperovals in the projective plane $\mathrm{PG}(2,q)$, q even. If q is odd, other lower bounds were known. In 1979, Sachar proved the following result for $\mathrm{C}(2,q)^\perp$.

THEOREM 4.4. [**44**, Proposition 2.3] *The minimum weight of $\mathrm{C}(2,q)^\perp$, $p > 2$, is at least $4q/3+2$.*

THEOREM 4.5. [**44**, Proposition 2.4] *Let c be a codeword of $\mathrm{C}(2,q)^\perp$, with $p \nmid wt(c)$. If $p = 5$, then $wt(c) \geq 4(2q+3)/5$ and if $p > 5$, then $wt(c) \geq (12q+18)/7$.*

The bounds derived by Sachar hold for the non-Desarguesian case as well. The divisibility condition in this latter theorem was proven to be unnecessary in [**35**], where the authors used the same ideas to extend these lower bounds to the code of $\mathrm{C}_k(n,q)^\perp$.

THEOREM 4.6. [**35**, Theorem 14][**35**, Theorem 15] *If $p \neq 2$, then $d(\mathrm{C}_t(n,q)^\perp) \geq (4\theta_{n-t}+2)/3$, if $p=7$, then $d(\mathrm{C}_t(n,q)^\perp) \geq (12\theta_{n-t}+2)/7$ and if $p>7$, then $d(\mathrm{C}_t(n,q)^\perp) \geq (12\theta_{n-t}+6)/7$.*

In 1999, Calkin, Key and de Resmini [**10**] extended Theorem 4.3 to general dimension.

THEOREM 4.7. [**10**, Proposition 1] *The minimum weight d of $\mathrm{C}_t(n,q)^\perp$ satisfies the following:*

$$(q+p)q^{n-t-1} \leq d \leq 2q^{n-t}.$$

They show again that for $p=2$, this lower bound is sharp.

THEOREM 4.8. [**10**, Theorem 1] *The minimum weight of $\mathrm{C}_t(n,q)^\perp$, q even, is $(q+2)q^{n-t-1}$.*

If $q=p$, it follows from Theorem 4.7 that the minimum weight of $\mathrm{C}_t(n,p)^\perp$ is $2p^{n-t}$. In [**35**], the authors derive this result in a different way; they show that finding the minimum weight of $\mathrm{C}_t(n,q)^\perp$ can be reduced to finding the minimum weight of $\mathrm{C}_1(n-t+1,q)^\perp$.

THEOREM 4.9. [**35**, Theorem 10] $d(\mathrm{C}_t(n,q)^\perp) = d(\mathrm{C}_1(n-t+1,q)^\perp)$.

Using Theorem 4.2 of Bagchi and Inamdar for $\mathrm{C}_1(n,p)^\perp$, p prime, they derive the following result for $\mathrm{C}_t(n,p)^\perp$. Note that it was already shown that the minimum weight of $\mathrm{C}_t(n,p)^\perp$ was $2p^{n-t}$, but the nature of the minimum weight codewords was not known.

THEOREM 4.10. [**35**, Theorem 12] *The minimum weight of $\mathrm{C}_t(n,p)^\perp$, p prime, is equal to $2p^{n-t}$, and the codewords of weight $2p^{n-t}$ are the scalar multiples of the difference of two $(n-t)$-spaces intersecting in an $(n-t-1)$-space.*

Bagchi and Inamdar conjecture that, if p is prime, the minimum weight of the dual code $\mathrm{C}_{s,t}(n,p)^\perp$ is $2p^{n-t}$ too and that the minimum weight codewords are exactly the ones constructed in the beginning of this section. Proving this is still an open problem, except for the cases $s=0$ and $t=s+1$.[**6**]

OPEN PROBLEM 4.11. Show that the minimum weight of $\mathrm{C}_{s,t}(n,p)^\perp$, p prime, equals $2p^{n-t}$ or construct a codeword of $\mathrm{C}_{s,t}(n,p)^\perp$ that has smaller weight.

OPEN PROBLEM 4.12. Determine the minimum weight of $\mathrm{C}_{s,t}(n,q)^\perp$.

4.2. A new upper bound on the minimum weight of $\mathrm{C}_k(n,q)^\perp$. When q is not a prime, there are counterexamples to Theorem 4.10 (with p replaced by q). In [**6**, p. 130], the authors write that they have no examples of codewords of $\mathrm{C}(2,q)^\perp$, with weight smaller than $2q$, where q is odd. The following theorem, proved in [**35**], provides numerous examples of such codewords for even and odd q.

THEOREM 4.13. [**35**, Theorem 13] *Let B be a minimal $(n-t)$-blocking set in $\mathrm{PG}(n,q)$ of size $q^{n-t}+x$, with $x<(q^{n-t}+1)/2$, such that there exists an $(n-t)$-space μ intersecting B in x points. The difference of the incidence vectors of B and μ is a codeword of $\mathrm{C}_k(n,q)^\perp$ of weight $2q^{n-t}+\theta_{n-t-1}-x$.*

PROOF. If $x < (q^{n-t}+1)/2$, then B is a small minimal $(n-t)$-blocking set, hence every t-space intersects B in 1 mod p points (see Theorem 2.1). If μ is an $(n-t)$-space π intersecting B in x points, then $(B-\mu,\pi) = (B,\pi)-(\mu,\pi) = 0$ for all t-spaces π since $(\mu,\pi) = 1$ and Theorem 2.1 shows that $(B,\pi) = 1$. Hence, $B-\mu$ is a codeword of $\mathrm{C}_t(n,q)^\perp$, with weight $|B|+\theta_{n-t}-2|B\cap\mu| = 2q^{n-t}+\theta_{n-t-1}-x$. □

We will use this theorem to improve on the upper bound for the minimum weight of codewords of $\mathrm{C}_t(n,q)^\perp$. To do this, we need to find a small minimal $(n-t)$-blocking set B of size $q^{n-t}+x$ such that there exists an $(n-t)$-space μ with $|\mu\cap B| = x$ where x is taken as large as possible. The following theorem corrects a wrong upper bound, derived by us earlier in [**35**, Theorem 13].

THEOREM 4.14. *There exists a small minimal $(n-t)$-blocking set B of size $q^{n-t}+x$ such that there is a $(n-t)$-space μ with $|B\cap\mu| = x$ and with $x = q^{n-t-1}(q-1)/(p-1)+\theta_{n-t-2}$.*

PROOF. Let B' be the set of points in $\mathrm{PG}(2,q)$ of the following form:

$$\{(1,x,x^p)|x\in\mathbb{F}_q\}\cup\{(0,x,x^p)|x\in\mathbb{F}_q\setminus\{0\}\}.$$

Now $\langle(0,x,x^p)\rangle = \langle(0,1,x^{p-1})\rangle$ and x^{p-1} takes $(q-1)/(p-1)$ different values, since $x^{p-1} = y^{p-1}$ if and only if $x = a\cdot y$ with $a\in\mathbb{F}_p\setminus\{0\}$. This implies that $|B'| = q+(q-1)/(p-1)$. The set B' is a blocking set of Rédei-type since the line L with equation $X_0 = 0$ contains $(q-1)/(p-1)$ points of B'. Embed $\nu = \mathrm{PG}(2,q)$ in $\mathrm{PG}(n-t+1,q)$ and let ψ be an $(n-t-2)$-dimensional space skew to ν. Let B be the cone with vertex ψ and base B', then B has size $q^{n-t-1}(q+(q-1)/(p-1))+\theta_{n-t-2} = q^{n-t}+x$ with $x = q^{n-t-1}(q-1)/(p-1)+\theta_{n-t-2}$. The $(n-t)$-space $\langle\psi,L\rangle$ meets B in x points. Embed $\mathrm{PG}(n-t+1,q)$ in $\mathrm{PG}(n,q)$. It is clear that the set B is a minimal $(n-t)$-blocking set in $\mathrm{PG}(n,q)$. □

Using this, together with Theorem 4.13, yields the following corollary.

COROLLARY 4.15. *The minimum weight of $\mathrm{C}_t(n,q)^\perp$ satisfies the following inequality:*

$$d(\mathrm{C}_t(n,q)^\perp) \le 2q^{n-t} - q^{n-t-1}(q-p)/(p-1).$$

For $n = 2$, i.e. the case of a Desarguesian projective plane, the codeword constructed was also found in [**29**].

4.3. The minimum weight of the hull. The *hull* of a linear code C is defined as $\mathrm{C}\cap\mathrm{C}^\perp$. The minimum weight vectors of the hull of $\mathrm{C}(2,q)$ are characterised in the following theorem.

THEOREM 4.16. [**2**, Corollary 6.4.4] *The hull $\mathrm{C}(2,q)\cap\mathrm{C}(2,q)^\perp$ has minimum weight $2q$ and the minimum weight vectors are the scalar multiples of the differences of the incidence vectors of any two distinct lines of $\mathrm{PG}(2,q)$.*

This was extended to the code of points and hyperplanes in [**34**].

THEOREM 4.17. [**34**, Theorem 5] *The minimum weight of the hull of $\mathrm{C}_{n-1}(n,q)$ is equal to $2q^{n-1}$.*

OPEN PROBLEM 4.18. Determine the minimum weight of the hull of the code $\mathrm{C}_{s,t}(n,q)$, where $(s,t)\neq(0,n-1)$.

4.4. The minimum weight of the dual code of a non-Desarguesian projective plane. As seen in Section 2.2, there exist non-Desarguesian projective planes, and also for these planes, the code of points and lines can be defined. The minimum weight of the dual code of a projective plane depends on the structure of this projective plane: projective planes of the same order can have dual codes with different minimum weights. The minimum weight of the dual code of arbitrary planes of orders $9, 25$ and 49, was studied, and for translation planes and Hughes planes, upper bounds on the minimum weight of the dual code were derived by constructing examples of small weight codewords.

As seen in Section 2.4, the smallest non-Desarguesian projective planes have order 9. For these cases, Key and de Resmini prove the following theorem.

THEOREM 4.19. [**27**] *Let* Π *be a projective plane of order 9. The minimum weight of the dual ternary code of* Π *is 15 if* Π *is* $\mathrm{PG}(2,9)$*, the Hall plane or the dual Hall plane, and 14 if* Π *is the Hughes plane.*

Clark, Key and de Resmini [**13**] proved the following result for planes of order 25.

THEOREM 4.20. [**13**] *If* Π *is a projective plane of order 25 and* C *is the code of* Π *over* $\mathbb{F}_5$*, then the minimum weight* d *of* $\mathrm{C}^{\perp}$ *is either* 42 *or* 44*, or* $45 \leq d \leq 50$*. Moreover,*

(1) *if* Π *has a Baer subplane, then the minimum weight is either 42, 44 or 45;*
(2) *if the minimum weight is 42, then a minimum weight word has a support that is the union of two projective planes,* π_1 *and* π_2*, of order 4 that are totally disjoint and the word has the form* $\pi_1 - \pi_2$*;*
(3) *if the minimum weight is 44, then the support of a minimum weight word is the union of two disjoint complete 22-arcs that have 11 2-secants in common;*
(4) *if the minimum weight is 45, then* $\pi - L$*, where* π *is a Baer subplane and* L *is a line of the subplane* π*, is a minimum weight word.*

In particular, the dual 5-ary code of the Desarguesian projective plane $\mathrm{PG}(2,25)$ *has minimum weight 45.*

For the dual 7-ary codes of the projective planes of order 49, the minimum weight is not known, but Ngwane and Key derived the following bounds.

THEOREM 4.21. [**30**] *If* C *is the 7-ary code of a projective plane of order 49, then the minimum weight* d *of* $\mathrm{C}^{\perp}$ *is in the range* $88 \leq d \leq 98$*. If the projective plane contains a Baer subplane, then* $88 \leq d \leq 91$*.*

For translation planes of order q^2 and q^3, the following theorem gives an upper bound on the minimum weight.

THEOREM 4.22. [**13**, Theorem 1] *Let* Π *be a projective translation plane of order* q^m*, where* $m = 2, 3$*,* $q = p^h$ *and* p *is prime. Then the dual code of the* p*-ary code of* Π *has codewords of weight* $2q^m - (q^{m-1} + q^{m-2} + \cdots + q)$*. If* Π *is Desarguesian, this also holds for* $m = 4$*.*

A similar construction to that used in the previous theorem was applied to Figueroa planes by Key and de Resmini in [**28**].

THEOREM 4.23. [**28**, Proposition 1] *Let* Π *be the Figueroa plane* $Fig(q^3)$ *where* $q = p^h$, p *prime. Let* C *denote the* p*-ary code of* Π. *Then* $\mathrm{C}^{\perp}$ *contains words of weight* $2q^3 - q^2 - q$. *Furthermore, if* d *denotes the minimum weight of* $\mathrm{C}^{\perp}$, *then*

(1) $d = q^3 + 2$ *if* $p = 2$,
(2) $\frac{4}{3}q + 2 \leq d \leq 2q^3 - q^2 - q$ *if* $p = 3$,
(3) $\frac{3}{2}q + 2 \leq d \leq 2q^3 - q^2 - q$ *if* $p > 3$.

OPEN PROBLEM 4.24. Determine the minimum weight of the dual code of other classes of projective planes.

OPEN PROBLEM 4.25. Derive a non-trivial upper bound on the minimum weight of the dual code of a projective plane that holds for arbitrary projective planes.

OPEN PROBLEM 4.26. Prove or disprove the conjecture that the minimum weight of the binary hull of a non-Desarguesian plane of order n is $2n$.

The previous conjecture is already proved in the Desarguesian case (see Theorem 4.16) and for the translation planes (see [**2**, p. 231]). If this were true in general, it would follow, if $n = 2 \mod 4$, $n > 2$, that there exist no hyperovals in this particular (putative) projective plane of order n (see [**4**, p. II-1]).

5. Summary

TABLE 1. Known values and bounds on the dimension and minimum weight of linear codes from projective spaces ($q = p^h$, p prime)

Code	dimension k	minimum weight d	Theorem
$\mathrm{C}_{s,t}(n,q)$		$\begin{bmatrix} t+1 \\ s+1 \end{bmatrix}_q$	3.1
$\mathrm{C}_t(n,q)$	See Theorems	θ_t	3.3,3.4
$\mathrm{C}_{n-1}(n,q)$	$\binom{n+p-1}{n}^h + 1$	θ_{n-1}	3.5
$\mathrm{C}_{s,s+2}(n,q)$	upper bound [**39**]	θ_s	
$\mathrm{C}_{s,t}(n,q)^\perp$		$2\left(\frac{q^{n-s}-1}{q^{t-s}-1}(1-\frac{1}{p})+\frac{1}{p}\right) \leq d$ $d \leq 2q^{n-t}$	 4.1
$\mathrm{C}_{s,s+1}(n,p)^\perp$		$2p^{n-s-1}$	4.1
$\mathrm{C}(2,q)^\perp$		$q+p \leq d \leq 2q$	4.3
$\mathrm{C}(2,q)^\perp$, $p>2$		$d \geq 4q/3+2$	4.4
$\mathrm{C}_t(n,q)^\perp$, $p>2$		$d \geq (4\theta_{n-t}+2)/3$	4.6
$\mathrm{C}_t(n,q)^\perp$		$(q+p)q^{n-t-1} \leq d \leq 2q^{n-t}$ $d = d(\mathrm{C}_1(n-t+1,q)^\perp)$	4.7 4.9
$\mathrm{C}_t(n,q)^\perp$, $p=2$		$(q+2)q^{n-t-1}$	4.8
$\mathrm{C}_t(n,p)^\perp$		$2p^{n-t}$	4.10
$\mathrm{C}_t(n,q)^\perp$		$d \leq 2q^{n-t} - q^{n-t-1}\frac{q-p}{p-1}$	4.15
$\mathrm{C}_{n-1}(n,q) \cap$ $\mathrm{C}_{n-1}(n,q)^\perp$		$2q^{n-1}$	4.17

References

[1] J. André. Über nicht-Desarguessche Ebenen mit transitiver Translationsgruppe. *Math. Z.* **60** (1954), 156–186.

[2] E.F. Assmus, Jr. and J.D. Key. Designs and their codes. *Cambridge University Press*, 1992.

[3] E.F. Assmus, Jr. and J.D. Key. Baer subplanes, ovals and unitals. Coding theory and design theory, Part I, 1–8, *IMA Vol. Math. Appl.* **20** Springer, New York, 1990.

[4] E.F. Assmus, Jr. and H.F. Mattson, Jr. *Algebraic theory of codes II.* Applied Research Laboratory, Sylvania Electronic Systems, 1969.

[5] R.D. Baker and K.L. Wantz. Unitals in the code of the Hughes plane. *J. Combin. Des.* **12** (2004), 35–38.

[6] B. Bagchi and S.P. Inamdar. Projective Geometric Codes. *J. Combin. Theory, Ser. A* **99** (2002), 128–142.

[7] A. Blokhuis, A.E. Brouwer, and H. Wilbrink. Hermitian unitals are code words. *Discrete Math.* **97** (1991), 63–68.

[8] R.C. Bose and R.C. Burton. A characterization of flat spaces in a finite geometry and the uniqueness of the Hamming and the MacDonald codes. *J. Combin. Theory* **1** (1966), 96–104.

[9] R.H. Bruck and R.C. Bose. The construction of translation planes from projective spaces. *J. Algebra* **1** (1964), 85–102.

[10] N.J. Calkin, J.D. Key, and M.J. de Resmini. Minimum weight and dimension formulas for some geometric codes. *Des. Codes Cryptogr.* **17** (1999), 105–120.

[11] K. Chouinard. Weight distributions of codes from planes (PhD Thesis, University of Virginia) (August 1998).
[12] K. Chouinard. On weight distributions of codes of planes of order 9. *Ars Combin.* **63** (2002), 3–13.
[13] K.L. Clark, L.D. Hatfield, J.D. Key, and H.N. Ward. Dual codes of projective planes of order 25. *Adv. Geom.* **3** (2003), 140–152.
[14] C.J. Colbourn and J.H. Dinitz (editors). Handbook of combinatorial designs. Discrete Mathematics and its Applications. *Chapman and Hall/CRC, Boca Raton*, 2007.
[15] V. Fack, Sz. Fancsali, L. Storme, G. Van de Voorde, and J. Winne. Small weight codewords in the codes arising from Desarguesian projective planes. *Des. Codes Cryptogr.* **46** (2008), 25–43.
[16] R. Figueroa. A family of not (v, ℓ)-transitive projective planes of order q^3, $q = 1 \mod 3$ and $q > 2$. *Math. Z.* **81** (1982), 471–479.
[17] A. Gacs, T. Szőnyi, and Zs. Weiner. Private communication (2009).
[18] J.M. Goethals and P. Delsarte. On a class of majority-logic decodable cyclic codes. *IEEE Trans. Inform. Theory* **14** (1968), 182–188.
[19] R.L. Graham and J. MacWilliams. On the number of information symbols in difference-set cyclic codes. *Bell System Tech. J.* **45** (1966), 1057–1070.
[20] N. Hamada. The rank of the incidence matrix of points and d-flats in finite geometries. *J. Sci. Hiroshima Univ. Ser. A-I* **32** (1968), 381–396.
[21] M. Hall, Jr. Uniqueness of the Projective Plane with 57 Points. *Proc. Amer. Math. Soc.***4(6)** (1953), 912–916.
[22] M. Hall, Jr., J.D. Swift, and R.J. Walker. Uniqueness of the projective plane of order eight. *Math. Tables Aids Comput.* **10**(1956), 186–194.
[23] D. Hilbert. The foundations of geometry (English translation of the 1899 original). Available online at *http://www.gutenberg.org/etext/17384*.
[24] J.W.P. Hirschfeld. Projective Geometries over Finite Fields. *Oxford University Press*, Oxford (1979).
[25] D.R. Hughes and F.C. Piper. Projective planes. *Springer-Verlag, New York*, 1973.
[26] S.P. Inamdar and N.S. Sastry. Codes from Veronese and Segre embeddings and Hamada's formula. *J. Combin. Theory Ser. A* **96(1)** (2001), 20–30.
[27] J.D. Key and M.J. de Resmini. Ternary dual codes of the planes of order nine. *J. Statist. Plan. Inference* **95** (2001), 229–236.
[28] J.D. Key and M.J. de Resmini. An upper bound for the minimum weight of dual codes of Figueroa planes. *J. Geom.* **77** (2003), 102–107.
[29] J.D. Key, T.P. McDonough, and V.C. Mavron. An upper bound for the minimum weight of the dual codes of Desarguesian planes. *European J. Combin.* **30** (2009), 220–229.
[30] J.D. Key and F. Ngwane. A lower bound for the minimum weight of the dual 7-ary code of a projective plane of order 49. *Des. Codes Cryptogr.* **44** (2007), 133–142.
[31] C.W.H. Lam. The search for a finite projective plane of order 10. *Amer. Math. Monthly* (1991), 305–318.
[32] C.W.H. Lam, S. Swiercz, and L. Thiel. The nonexistence of finite projective planes of order 10. *Canad. J. Math.* **41(6)** (1989), 1117–1123.
[33] C.W.H. Lam, G. Kolesova, and L. Thiel. A computer search for finite projective planes of order 9. *Discrete Math.* **92** (1991), 187–195.
[34] M. Lavrauw, L. Storme, and G. Van de Voorde. On the code generated by the incidence matrix of points and hyperplanes in PG(n, q) and its dual. *Des. Codes Cryptogr.* **48** (2008), 231–245.
[35] M. Lavrauw, L. Storme, and G. Van de Voorde. On the code generated by the incidence matrix of points and k-spaces in PG(n, q) and its dual. *Finite Fields Appl.* **14** (2008), 1020–1038.
[36] M. Lavrauw, L. Storme, P. Sziklai, and G. Van de Voorde. An empty interval in the spectrum of small weight codewords in the code from points and k-spaces of PG(n, q). *J. Combin. Theory, Ser. A* **116** (2009), 996–1001.
[37] J.H. Maclagan-Wedderburn. A Theorem on Finite Algebras. *Trans. Amer. Math. Soc.* **6** (1905), 349–352.
[38] F.J. MacWilliams and N.J.A. Sloane. The theory of error-correcting codes. *North-Holland Mathematical Library*, Amsterdam-New York-Oxford (1977).

[39] P. McClurg. On the rank of certain incidence matrices over GF(2). *European J. Combin.* **20** (1999), 421–427.
[40] G. McGuire and H. Ward. The weight enumerator of the code of the projective plane of order 5. *Geom. Dedicata* **73** (1998), no. 1, 63–77.
[41] T.G. Ostrom. Derivable nets. *Canad. Math. Bull.* **8** (1965), 601–613.
[42] T. Penttila, G. Royle. Classification of hyperovals in PG$(2, 32)$. *J. Geom.* **50(1–2)** (1994), 151–158.
[43] E. Prange. The use of coset equivalence in the analysis and decoding of group codes, TN-59-16, Air Force Cambridge Research Labs, Bedford, MA, 1959.
[44] H. Sachar. The $\mathbb{F}_p$ span of the incidence matrix of a finite projective plane. *Geom. Dedicata* **8** (1979), 407–415.
[45] C.J. Salwach. Planes, biplanes, and their codes. *Amer. Math. Monthly* **88(2)** (1981), 106–125.
[46] B. Segre. Sulle ovali nei piani lineari finiti. *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat. (8)* **17** (1954), 141–142.
[47] B. Segre. Teoria di Galois, fibrazioni proiettive e geometrie non desarguesiane. *Ann. Mat. Pura Appl.(4)* **64** (1964), 1–76.
[48] P. Sin. The p-rank of the incidence matrix of intersecting linear subspaces. *Des. Codes Cryptogr.* **31** (2004), 213–220.
[49] T. Szőnyi and Zs. Weiner. Small blocking sets in higher dimensions. *J. Combin. Theory, Ser. A* **95** (2001), 88–101.
[50] O. Veblen and J.H Maclagan-Wedderburn. Non-Desarguesian and non-Pascalian geometries. *Trans. Amer. Math. Soc.* **8** (1907), 279–388.

Department of pure mathematics and computer algebra, Ghent University, Krijgslaan 281-S22, 9000 Ghent (Belgium)
E-mail address: {ml,ls,gvdvoorde}@cage.ugent.be